IT Security Automation Conference (ITSAC)

Tom Millar (DHS), Joe Jarzombek (DHS), Steve Quinn (NIST), Richard Struse (DHS), and MITRE and NIST staff will be speaking at ITSAC on October 31. To better enable software stakeholders to reduce risks attributable to the most significant exploitable software errors relevant to specific business/mission domains and technologies, DHS NCSD SwA program has sponsored the development of the Common Weakness Risk Analysis Framework (CWRAF). The CWRAF uses the Common Weakness Scoring System (CWSS) scoring criteria with CWE to provide consistent measures for prioritizing risk mitigation efforts and focusing secure coding practices, enabling better informed decision-making for the development and acquisition of more resilient software products and services.

CWRAF enables more targeted specification of "Top-N" CWE lists that are relevant to specified technologies used within specific business domains. In the past, the Top 25 CWE lists have represented community collaboration efforts to prioritize the most exploitable constructs that make software vulnerable to attack or failure. Now with CWRAF, business domains can use the scoring criteria with CWE to identify exploitable software fault patterns that are most significant to them in specific technologies: web applications, control systems, embedded systems, end-point computing devices, operating systems, databases, storage systems, enterprise system applications, and cloud computing services. In this workshop, participants will construct one or more CWRAF "vignettes" for specific business domains. As each vignette is built and refined, we will automatically recalculate the scores for the entire CWE database, allowing participants to understand how the decisions made during vignette definition affect the assessment of risk for individual weaknesses. Input from attendees will be used to continue to refine the concepts in CWRAF and identify business domains and technology areas that would benefit from CWRAF.

The National Institute of Standards and Technology, in conjunction with the Department of Homeland Security, National Security Agency, and Defense Information Systems Agency, will host the 7th Annual IT Security Automation Conference.

The Security Content Automation Protocol (SCAP) community is a public/private partnership consisting of interested parties from industry, research, and educational institutions and government that are working to advance automation and standardization of technical security operations.

Date: October 31-November 2, 2011

Location: Hyatt Regency Crystal City | Arlington, Virginia

Additional information is forthcoming. Please check for updates at http://scap.nist.gov/events.